Privacy requirements: LINDDUN PRO

Introduction: Open Mind Vault

"Open Mind Vault" is a SAPUI5 application hosted in a launchpad, designed to serve as a platform for users to capture and organize their thoughts. The application consists of both a frontend and a backend, with the database primarily functioning as a cache due to certain limitations. To ensure secure access, the application integrates with Identity Provider (IDP) via the XSUAA service. Users log in through this service, gaining access to the launchpad and subsequently, the Open Mind Vault app.

**User Flow:**

1. User A accesses the launchpad by navigating to: [Home](https://a8462f3ftrial.launchpad.cfapps.us10.hana.ondemand.com/site?siteId=137c66b4-7048-421f-b0fc-2645bd06c0d0#Shell-home).
2. If not logged in, the user is redirected to the IDP through the XSUAA service for authentication:

A screenshot of a computer

Description automatically generated

1. Upon successful login, the user gains access to the launchpad:

A close-up of a computer screen

Description automatically generated

1. Within the launchpad, the Open Mind Vault app is available for selection.
2. Clicking on the Open Mind Vault app opens the application's interface:

A white rectangular box with text

Description automatically generated

**Application Features:**

* Users can create entries in the Open Mind Vault.
* Entries can be marked as public or private, offering customization in sharing thoughts.

A screenshot of a computer

Description automatically generated

**Note**:

Accessing SAPUI5 apps or the backend API directly, without going through the Launchpad (by manipulating URLs), will trigger a login process. These components are protected by XSUAA service, necessitating authentication for secure interaction.

All communication/data flow is safeguarded through encryption (https).

Data Flow Diagram

A diagram of a business process

Description automatically generated

LINDDUN Mapping table

A table with black and white text

Description automatically generated

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Threat Target** | | | | | | |
|  | **Interaction** | | | **Source** | **Destination** | **Row in mapping table** |
| **DF1** | **Client** | **🡪** | **Launchpad** | **External Entity** | **Process** | **5** |
| **DF2** | **Launchpad** | **Client** | **Process** | **External Entity** | **3** |
| **DF3** | **Launchpad** | **XSUAA** | **Process** | **Process** | **1** |
| **DF4** | **XSUAA** | **Launchpad** | **Process** | **Process** | **1** |
| **DF5** | **XSUAA** | **IDP** | **Process** | **External Entity** | **3** |
| **DF6** | **IDP** | **XSUAA** | **External Entity** | **Process** | **5** |
| **DF7** | **Launchpad** | **SAPUI5** | **Process** | **Process** | **1** |
| **DF8** | **SAPUI5** | **Launchpad** | **Process** | **Process** | **1** |
| **DF9** | **SAPUI** | **XSUAA** | **Process** | **Process** | **1** |
| **DF10** | **XSUAA** | **SAPUI5** | **Process** | **Process** | **1** |
| **DF11** | **SAPUI** | **Backend** | **Process** | **Process** | **1** |
| **DF12** | **Backend** | **SAPUI5** | **Process** | **Process** | **1** |
| **DF13** | **Backend** | **XSUAA** | **Process** | **Process** | **1** |
| **DF14** | **XSUAA** | **Backend** | **Process** | **Process** | **1** |
| **DF15** | **Backend** | **Database** | **Process** | **Data Store** | **2** |
| **DF16** | **Database** | **Backend** | **Data Store** | **Process** | **4** |

**Data involved:**

In the app, the only information used are users “thoughts”. This includes a title, description, and the author's email address (which is derived from the user token in the backend).

**Note:**

Data flows 9,10,13 & 14 will not be discussed as they are identical to data flow 3 & 4

LINDDUN Threat trees

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A yellow and white rectangular box with black text

Description automatically generated

A screenshot of a computer

Description automatically generated

## DF1 Client request launchpad (and apps) via https





### Linking:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **L** | **I** | **NR** | **D** | **DD** | **U** | **NC** |
| **Source** | / | I.1.1  I.2.1.1 | Nr.1.1 | / | / | U.2.1  U.2.3 |  |
| **Flow** | / | / | / | / | / |  |  |
| **Destination** | / | / | / |  | / | / | / |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Source** | **Flow** | **Destination** | **Location** | **Characteristics** | **Description** |
| E1 | DF1 | P1 | E1 | I.1.1, I.2.1.1 | The author is prefilled when returning thoughts. The email address is used as the author attribute. |
| E1 | DF1 | P1 | E1 | Nr.1.1 | The accountability of the content of a thought is ensured since the author is linked to the email address. |
| E1 | DF1 | P1 | E1 | U.2.1, U.2.3 | Lack of consent and feature to erase/correct data |

## DF2 Launchpad sends back HTML5 page and assets to the client





### Linking:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **L** | **I** | **NR** | **D** | **DD** | **U** | **NC** |
| **Source** | / | / | / | / | / | / | / |
| **Flow** | / | / | / | / | / |  |  |
| **Destination** | / | / | / |  | / | / | / |

## DF3 Launchpad authenticate user via XSUAA service





### Linking:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **L** | **I** | **NR** | **D** | **DD** | **U** | **NC** |
| **Source** | / | / | / | / | / | / | / |
| **Flow** | / | / | / | / | / |  |  |
| **Destination** | / | / | / |  | / | / | / |

## DF4 XSUAA service responds with authentication response





### Linking:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **L** | **I** | **NR** | **D** | **DD** | **U** | **NC** |
| **Source** | / | / | / | / | / | / | / |
| **Flow** | / | / | / | / | / |  |  |
| **Destination** | / | / | / |  | / | / | / |

## DF5 XSUAA service reaches out the IDP for authentication





### Linking:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **L** | **I** | **NR** | **D** | **DD** | **U** | **NC** |
| **Source** | / | / | / | / | / | / | / |
| **Flow** | / | / | / | / | / |  |  |
| **Destination** | / | / | / |  | / | / | / |

## DF6 IDP authenticate user (if present in the user store)





### Linking:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **L** | **I** | **NR** | **D** | **DD** | **U** | **NC** |
| **Source** | / | / | / | / | / | / |  |
| **Flow** | / | / | / | / | / |  |  |
| **Destination** | / | / | / |  | / | / | / |

## DF7 Launchpad fetches SAPUI5 apps from the HTML5 repository



### Linking:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **L** | **I** | **NR** | **D** | **DD** | **U** | **NC** |
| **Source** | / | / | / | / | / | / | / |
| **Flow** | / | / | / | / | / |  |  |
| **Destination** | / | / | / |  | / | / | / |

## DF8 HTML5 repository serves the launchpad the SAPUI5 apps





### Linking:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **L** | **I** | **NR** | **D** | **DD** | **U** | **NC** |
| **Source** | / | / | / | / | / | / | / |
| **Flow** | / | / | / | / | / |  |  |
| **Destination** | / | / | / |  | / | / | / |

## DF11 SAPUI5 app request and post data to the backend





### Linking:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **L** | **I** | **NR** | **D** | **DD** | **U** | **NC** |
| **Source** | / | I.1.1  I.2.1.1 | Nr.1.1 | / | / | U.2.1  U.2.3 | / |
| **Flow** | / | / | / | / | / |  |  |
| **Destination** | / | / | / |  | / | / | / |

When accessing the SAPUI5 apps directly, the same threats can be observed as with the launchpad.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Source** | **Flow** | **Destination** | **Location** | **Characteristics** | **Description** |
| P3 | DF11 | P4 | P3 | I.1.1, I.2.1.1 | The author is prefilled when returning thoughts. The email address is used as the author attribute. |
| P3 | DF11 | P4 | P3 | Nr.1.1 | The accountability of the content of a thought is ensured since the author is linked to the email address. |
| P3 | DF11 | P4 | P3 | U.2.1, U.2.3 | Lack of consent and feature to erase/correct data |

## DF12 Backend treats the SAPUI5 requests





### Linking:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **L** | **I** | **NR** | **D** | **DD** | **U** | **NC** |
| **Source** | / | / | / | / | / | / | / |
| **Flow** | / | / | / | / | / |  |  |
| **Destination** | / | / | / |  | / | / | / |

## DF15 Backend fetches/insert data from/into database





### Linking:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **L** | **I** | **NR** | **D** | **DD** | **U** | **NC** |
| **Source** | / | I.1.1  I.2.1.1 | / | / | / | U.2.3 | / |
| **Flow** | / | / | / | / | / |  |  |
| **Destination** | / | / | / |  | / | / | Nc.1.1.1,Nc.1.1.4  Nc.1.1.3.1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Source** | **Flow** | **Destination** | **Location** | **Characteristics** | **Description** |
| P4 | DF15 | DS1 | P4 | I.1.1, I.2.1.1 | The author is prefilled when returning thoughts. The email address is used as the author attribute. |
| P4 | DF15 | DS1 | P4 | U.2.3 | Lack of feature to erase/correct data |
| P4 | DF15 | DS1 | DS1 | Nc.1.1.1,Nc.1.1.4,  Nc.1.1.3.1 | Non-compliance is observed as the data stored cannot be controlled (erased/corrected), nor the amount of time it persists in the system. Consent is non existing. |

## DF16 Database returns transaction result to backend





### Linking:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **L** | **I** | **NR** | **D** | **DD** | **U** | **NC** |
| **Source** | / | / | / | / | / | / | / |
| **Flow** | / | / | / | / | / |  |  |
| **Destination** | / | / | / |  | / |  | / |

Privacy threats

|  |  |
| --- | --- |
| **Number** | T1 |
| **Title** | Automated Attribution |
| **Summary** | The author is prefilled when returning thoughts. The email address is used as the author attribute. |
| **DFD Elements** | E1 (client), DF1, P1 (launchpad) |
| **Threat Type** | IDENTIFYING |
| **Tree nodes** | I.1.1, I.2.1.1 |
| **Assets involved** | User Email address |
| **Priority** | LOW |
| **Comments** | We should provide a way for users to use a username instead |

|  |  |
| --- | --- |
| **Number** | T2 |
| **Title** | Ensuring Thought Accountability: Author-Email Linkage for Content Integrity |
| **Summary** | The accountability of the content of a thought is ensured since the author is linked to the email address. |
| **DFD Elements** | E1 (client), DF1, P1 (launchpad) |
| **Threat Type** | NON REPUDIATION |
| **Tree nodes** | Nr.1.1 |
| **Assets involved** | User Email address |
| **Priority** | LOW |
| **Comments** | We should provide a way for users to use a username instead |

|  |  |
| --- | --- |
| **Number** | T3 |
| **Title** | Empowering Control |
| **Summary** | Lack of consent and feature to erase/correct data |
| **DFD Elements** | E1 (client), DF1, P1 (launchpad) |
| **Threat Type** | UNAWARENESS, UNINTERVENABILITY |
| **Tree nodes** | U.2.1, U.2.3 |
| **Assets involved** |  |
| **Priority** | HIGH |
| **Comments** | Consent need to be enforced as well as a way to erase/correct data |

(Note T1-T3 can be applied as well for the SAPUI5 apps)

|  |  |
| --- | --- |
| **Number** | T4 |
| **Title** | Automated Attribution |
| **Summary** | The author is prefilled when returning thoughts. The email address is used as the author attribute. |
| **DFD Elements** | P4 (backend), DF15, DS1 (database) |
| **Threat Type** | IDENTIFYING |
| **Tree nodes** | I.1.1, I.2.1.1 |
| **Assets involved** | User Email address |
| **Priority** | LOW |
| **Comments** | We should provide a way for users to use a username instead |

|  |  |
| --- | --- |
| **Number** | T5 |
| **Title** | Empowering Control |
| **Summary** | Lack of feature to erase/correct data |
| **DFD Elements** | P4 (backend), DF15, DS1 (database) |
| **Threat Type** | UNAWARENESS, UNINTERVENABILITY |
| **Tree nodes** | U.2.3 |
| **Assets involved** |  |
| **Priority** | HIGH |
| **Comments** | The backend should provide a way to correct/delete stored data |

|  |  |
| --- | --- |
| **Number** | T6 |
| **Title** | Unraveling Non-Compliance |
| **Summary** | Non-compliance is observed as the data stored cannot be controlled (erased/corrected), nor the amount of time it persists in the system. Consent is non existing. |
| **DFD Elements** | P4 (backend), DF15, DS1 (database) |
| **Threat Type** | UNAWARENESS, UNINTERVENABILITY |
| **Tree nodes** | Nc.1.1.1,Nc.1.1.4,Nc.1.1.3.1 |
| **Assets involved** |  |
| **Priority** | HIGH |
| **Comments** | Compliance with regulation need to be respected and enforced. |